2011 CyberSecurity Watch Survey

How Bad Is the Insider Threat?

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **JAN 2011**	2. REPORT TYPE	3. DATES COVERED **00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE
2011 CyberSecurity Watch Survey: How Bad Is the Insider Threat?

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Carnegie Mellon University,Software Engineering Institute,Pittsburgh,PA,15213

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The Insider Threat team has teamed with the U.S. Secret Service and CSO magazine to conduct, analyze, and publish findings from an annual CyberSecurity Watch Survey from research that was conducted to attempt to identify electronic crime fighting trends and techniques, including best practices and emerging trends.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**8**	

NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN “AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

2011 CyberSecurity Watch Survey -1

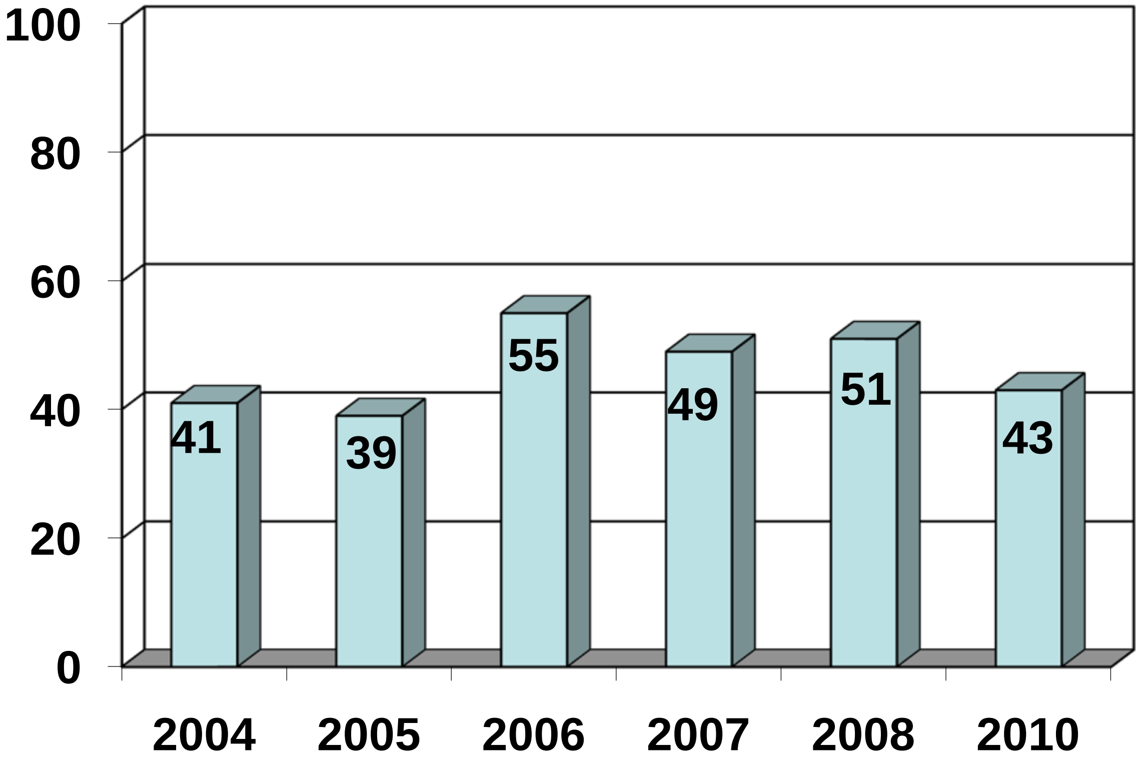
CSO Magazine, USSS, CERT & Deloitte

607 respondents

38% of organizations have more than 5000 employees

37% of organizations have less than 500 employees

Percentage of Participants Who Experienced an Insider Incident



Source: 2011 CyberSecuirty Watch Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, January 2011.

2011 CyberSecurity Watch Survey -2

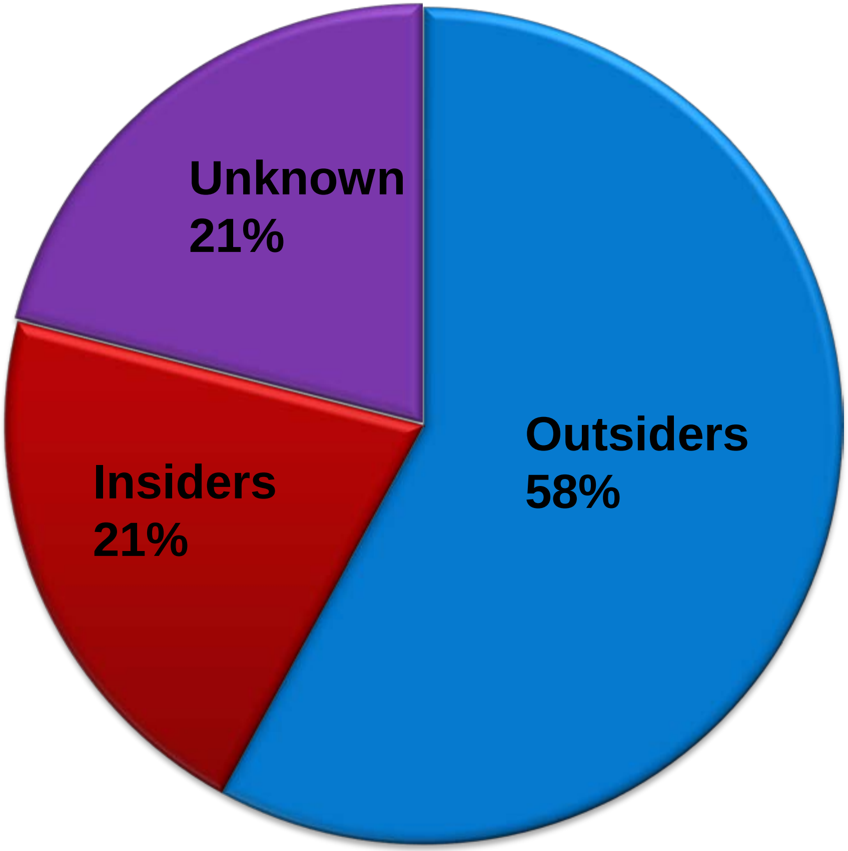
46 % of respondents	Damage caused by insider attacks more damaging than outsider attacks
Most common insider e-crime	

Unauthorized access to / use of corporate information	(63%)
Unintentional exposure of private or sensitive data	(57%)
Virus, worms, or other malicious code	(37%)
Theft of intellectual property	(32%)

Source: 2011 CyberSecuirty Watch Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, January 2011.

2011 CyberSecurity Survey Results -1

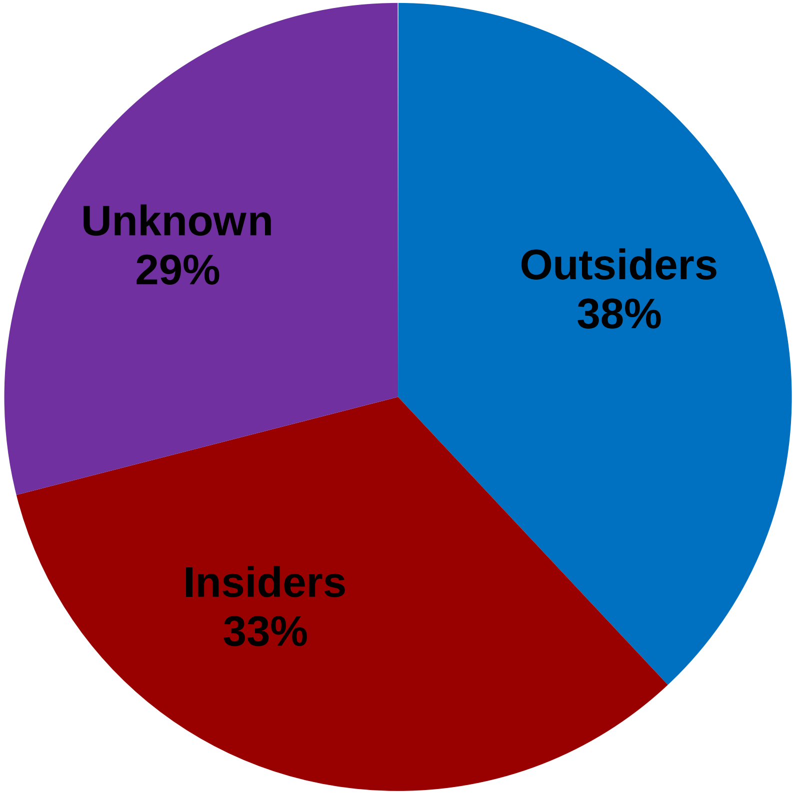
What percent of the Electronic Crime events are known or suspected to have been caused by :



Source: 2011 CyberSecuirty Watch Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, January 2011.

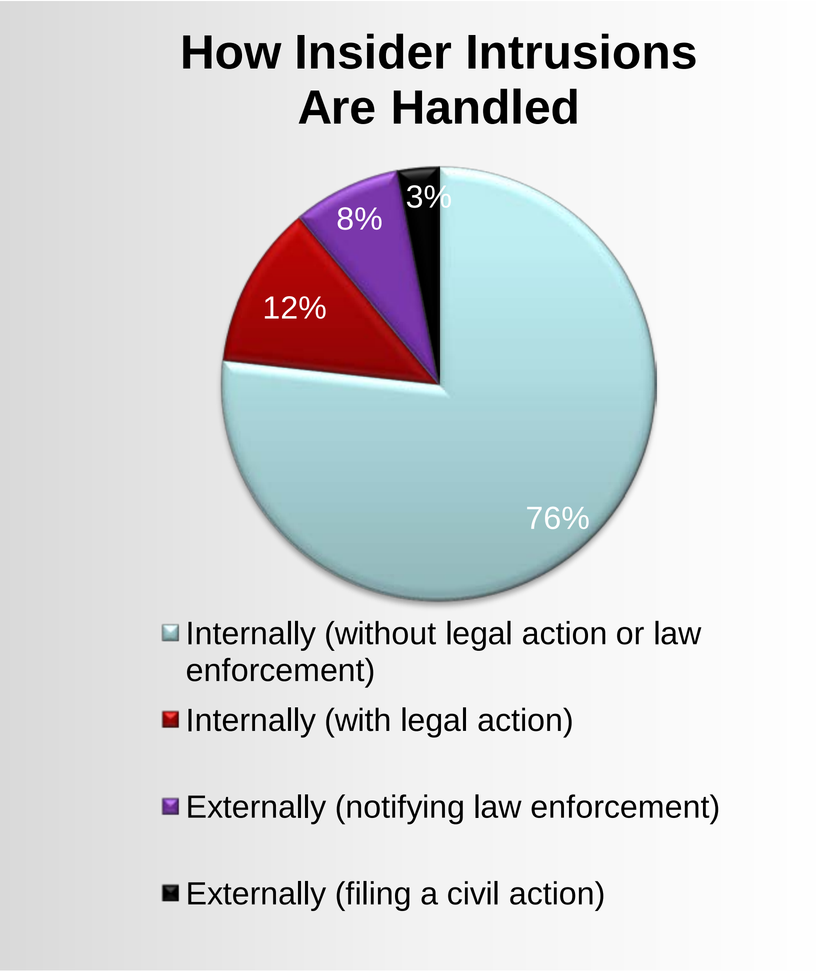
2011 CyberCrime Survey Results - 2

Which Electronic Crimes were more costly or damaging to your organization, those perpetrated by:



Source: 2011 CyberSecuirty Watch Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, January 2011.

2011 CyberCrime Survey Results - 3



How Insider Intrusions Are Handled

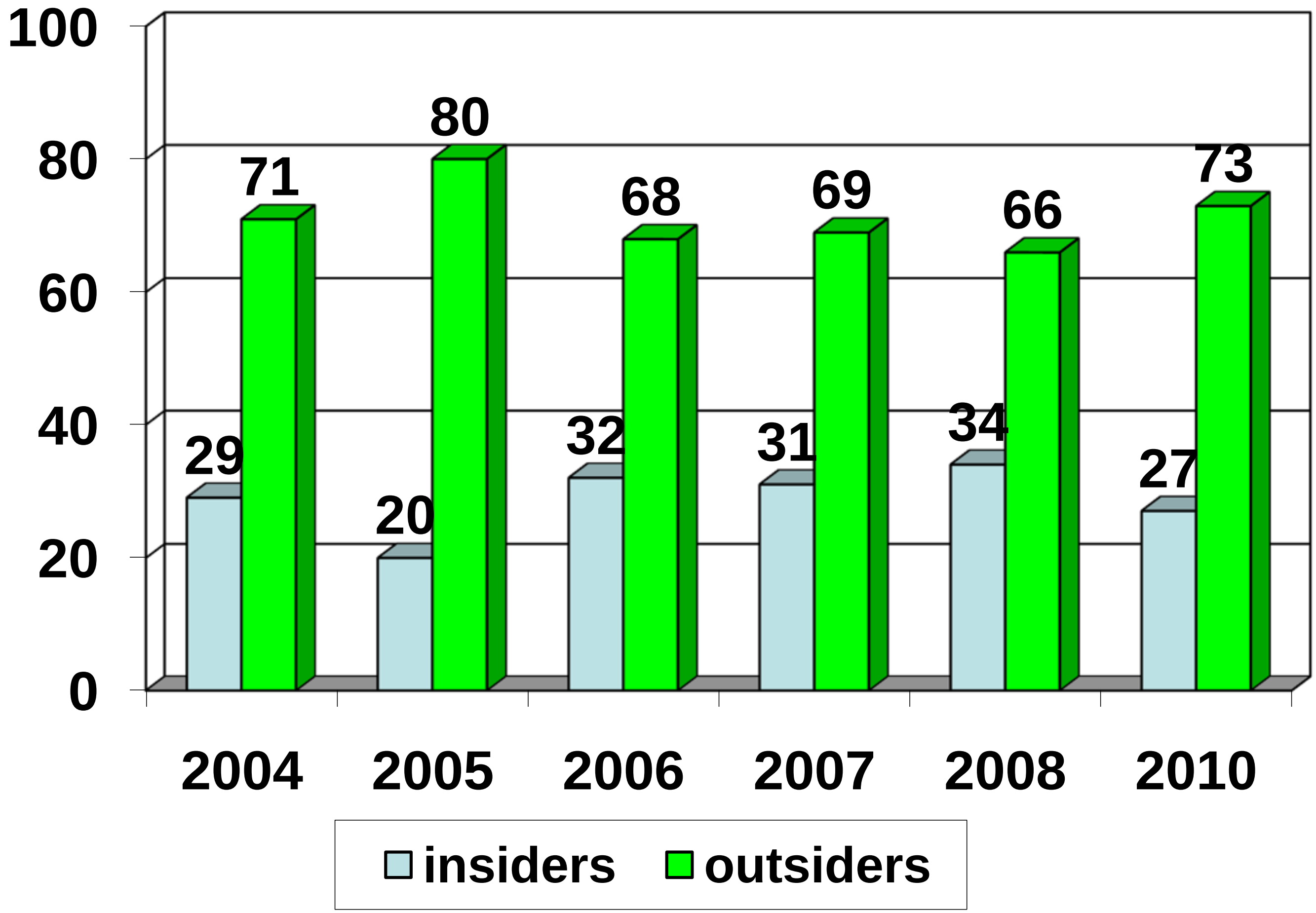
Reason(s) CyberCrimes were not referred for legal action

	2011	2010
Damage level insufficient to warrant prosecution	42%	37%
Could not identify the individual/ individuals responsible for committing the eCrime	40%	29%
Lack of evidence/not enough information to prosecute	39%	35%
Concerns about negative publicity	12%	15%
Concerns about liability	8%	7%
Concerns that competitors would use incident to their advantage	6%	5%
Prior negative response from law enforcement	5%	7%
Unaware that we could report these crimes	4%	5%
Other	11%	5%
Don't know	20%	14%
Not applicable	N/A	24%

Source: 2011 CyberSecuirty Watch Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, January 2011.

2011 CyberCrime Survey Results - 4

Percentage of insiders versus outsiders



Source: 2011 CyberSecuirty Watch Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, January 2011.